Available online at www.sciencedirect.com
SCIENCE DIRECT®
Finite Fields and Their Applications 9 (2003) 423–431
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

On computation of the greatest common divisor of several polynomials over a finite field

Alessandro Conflitti

Dipartimento di Matematica, Università degli Studi di Roma "Tor Vergata", Via della Ricerca Scientifica, I-00133 Roma, Italy

Received 6 February 2002; revised 3 February 2003; accepted 9 April 2003

Communicated by Gary L. Mullen

Abstract

We propose a probabilistic algorithm to reduce computing the greatest common divisor of m polynomials over a finite field (which requires computing $m-1$ pairwise greatest common divisors) to computing the greatest common divisor of two polynomials over the same field.

Keywords: Polynomials over a finite field; Greatest common divisor; Probabilistic algorithm

1. Overview

In this paper we show that the ideas of the paper [2], which exhibits a probabilistic algorithm that calculates the gcd of many integers using gcd's of pairs of integers, can be applied to the computation of the greatest common divisor of several polynomials over finite fields. Moreover, as one might expect, the analysis of this algorithm (for polynomials over a finite field) is considerably simpler and tighter than the algorithm of [2] for the integers.

Let q be a prime power and let $\mathbb{F}_q$ denote the finite field of q elements.

Given m non-zero polynomials $a_1, \ldots, a_m \in \mathbb{F}_q[X]$ we define

$$d = \gcd(a_1, \ldots, a_m)$$

as the unique monic polynomial $d \in \mathbb{F}_q[X]$ of the largest possible degree, which divides each polynomial $a_1, \ldots, a_m$.

E-mail address: conflitt@mat.uniroma2.it.

1071-5797/03/$ - see front matter
doi:10.1016/S1071-5797(03)00022-4

We show that following the ideas of the paper [2] one can design a simple probabilistic algorithm which, for a fixed q reduces the original problem to compute the greatest common divisor of a pair of polynomials.

In order to deterministically compute $\gcd(a_1, \ldots, a_m)$ we need to perform $m-1$ pairwise greatest common divisors, i.e. $A_{j+1} = \gcd(A_j, a_{j+1})$ for $1 \leqslant j \leqslant m-1$, with $A_1 = a_1$, and of course $A_m = \gcd(a_1, \ldots, a_m)$.

The ideas of this paper in order to compute the greatest common divisor of $a_1, \ldots, a_m$ is to select $2m$ random polynomials $u_1, \ldots, u_m, v_1, \ldots, v_m \in \mathbb{F}_q[X]$ with the same degree s and perform

$$D = \gcd\left(\sum_{j=1}^{m} u_j a_j, \sum_{j=1}^{m} v_j a_j \right).$$

It is clear that D is a multiple of $\gcd(a_1, \ldots, a_m)$: we prove that with high probability D is exactly $\gcd(a_1, \ldots, a_m)$. More exactly, we prove that for any $q \geqslant 3$ the probability of success is always greater than $\frac{1}{2}$, and even when $q = 2$ it is greater than $\frac{3}{10}$. Moreover, if $q = 2$ executing our algorithm twice we have that the probability of success becomes greater than $\frac{51}{100}$.

We remark, that yet another way of reduction of the computing the greatest common divisor of several polynomials to computing of the greatest common divisor of a pair of polynomials, see Section 6.9 of [3] (as well as [2]). However for small values of q (for example, for $q = 2$ or $q = 3$) this requires computing the greatest common divisor over an appropriate extension of the ground field $\mathbb{F}_q$ which may not be available in the selected computational model, say if computation of the greatest common divisor is given as a black-box algorithm. In any case, working in extension fields is computationally more expensive.

Furthermore, there are also a couple of methods which avoid extension field, see [5,6]. However, in order to guarantee a non-trivial result (i.e. the probability of success greater than $\frac{1}{2}$), the method of [5] requires the computation of $\log_2(2n)$ pairwise greatest common divisors, where n is an upper bound for the degree of the polynomials $a_1, \ldots, a_m$, and the algorithm proposed in [6] requires the computation of 6 pairwise greatest common divisors if $q \geqslant 3$ and the computation of 14 pairwise greatest common divisors if $q = 2$.

Instead, the algorithm of this paper requires the computation of only one pairwise greatest common divisor if $q \geqslant 3$, and of two pairwise greatest common divisors if $q = 2$. Moreover, our analysis allows us to prove a described positive probability of success even computing only one pairwise greatest common divisor.

We present a more detailed comparison of all these approaches.

Throughout the paper $\log z$ denotes the natural logarithm of z; constants in the "O"-symbol are absolute.

2. Main result

Let $q \geqslant 2$ and

$$\gamma(q) = \sum_{k=1}^{\infty} I_k q^{-2k},$$

where I_k is the number of monic irreducible polynomial of degree k. It is well known that

$$I_k = \frac{1}{k} \sum_{r|k} \mu(r) q^{\frac{k}{r}}, \tag{1}$$

where $\mu(r)$ is the Möbius function, see [4].

We also denote by $\mathscr{M}_k$ the set of all monic polynomials over $\mathbb{F}_q[X]$ of degree $k \geqslant 1$.

We consider polynomials $a_1, \ldots, a_m \in \mathbb{F}_q[X]$ of degree at most n such that the maximum degree is taken by only one polynomial, viz. rearranging $a_1, \ldots, a_m$ by degree we have $\deg a_1 > \deg a_j$, $j = 2, \ldots, m$.

We remark that this is not a restricted hypothesis, because as in Section 8.9 of [1] if $\deg a_1 = \deg a_2 \geqslant \deg a_j$, $j = 3, \ldots, m$ we can replace a_1 with $X \cdot a_2 + a_1$.

Theorem 1. *Let $m, s \geqslant 1$ be integers and $a_1, \ldots, a_m \in \mathbb{F}_q[X]$ non-zero polynomials of degree at most n such that the maximum degree is taken by only one polynomial. For $u_1, \ldots, u_m, v_1, \ldots, v_m$ selected independently and uniformly at random from $\mathscr{M}_s$, let P be the probability that*

$$\gcd\left(\sum_{j=1}^{m} u_j a_j, \sum_{j=1}^{m} v_j a_j \right) = \gcd(a_1, \ldots, a_m).$$

Then

$$P \geqslant 1 - \gamma(q) - \frac{n+s}{s} q^{-s}.$$

Proof. As in [2], we remark that it is enough to consider the case where $a_1, \ldots, a_m$ are relatively prime.

Denote by T the number of sequences of polynomials $u_j, v_j \in \mathscr{M}_s$, $j = 1, \ldots, m$ with

$$\gcd\left(\sum_{j=1}^{m} u_j a_j, \sum_{j=1}^{m} v_j a_j \right) = 1.$$

Thus

$$P = T q^{-2sm}.$$

Denote by $\mathscr{I}_k$ the set of monic irreducible polynomials of degree k over $\mathbb{F}_q$, so that $I_k = \#\mathscr{I}_k$. Obviously

$$T \geqslant q^{2sm} - \sum_{k=1}^{n+s} \sum_{f \in \mathscr{I}_k} N_f^2,$$

where N_f is the number of $(w_1, \ldots, w_m) \in \mathscr{M}_s^m$ for which f divides

$$w = \sum_{j=1}^{m} w_j a_j.$$

Therefore

$$T \geqslant q^{2sm} - S - R,$$

where

$$S = \sum_{k=1}^{s-1} \sum_{f \in \mathscr{I}_k} N_f^2 \quad \text{and} \quad R = \sum_{k=s}^{n+s} \sum_{f \in \mathscr{I}_k} N_f^2.$$

Because $\gcd(a_1, \ldots, a_m) = 1$, for every $f \in \mathscr{I}_k$ with $1 \leqslant k \leqslant n+s$ there exists some $j_0 \leqslant m$ with $f \nmid a_{j_0}$. Then, if $f \mid w$, from the congruence

$$w_{j_0} a_{j_0} \equiv -\sum_{\substack{j=1 \\ j \neq j_0}}^{m} w_j a_j \pmod{f},$$

we conclude that for any values of w_j, for $j \neq j_0$, the polynomial w_{j_0} is uniquely determined modulo f. Therefore

$$N_f = q^{sm - \deg f} \tag{2}$$

if $\deg f \leqslant s-1$, and

$$N_f \leqslant q^{sm-s} \tag{3}$$

if $\deg f \geqslant s$. Then for the sum S we derive from (2)

$$S = \sum_{k=1}^{s-1} I_k q^{2sm-2k} \leqslant q^{2sm} \gamma(q).$$

To estimate the sum R, we remark that bound (3) implies

$$R \leqslant q^{sm-s} \sum_{k=s}^{n+s} \sum_{f \in \mathscr{I}_k} N_f = q^{sm-s} W,$$

where W is the total number of irreducible divisors of degree at least s (counted with their multiplicity) of the polynomial

$$Q = \prod_{w_1,\dots,w_m \in \mathcal{M}_s} \sum_{j=1}^{m} a_j w_j.$$

We remark that $Q \neq 0$, because the maximum degree of $a_1, \dots, a_m$ is taken by only one polynomial a_j.

Then we derive

$$W \leqslant \frac{1}{s} \deg Q \leqslant \frac{n+s}{s} q^{sm}$$

and the desired result follows. □

In particular, if $s \geqslant 1 + \log_q n$ we obtain $P \geqslant 1 - \gamma(q) - 2s^{-1}q^{-1}$.

Now we give an upper bound for $\gamma(q)$.

Theorem 2. *The bound*

$$\gamma(q) \leqslant \log\left(\frac{q}{q-1}\right)$$

holds for any $q \geqslant 2$.

Proof. From (1) we derive

$$\gamma(q) = \sum_{k=1}^{\infty} I_k q^{-2k} = \sum_{k=1}^{\infty} \frac{1}{kq^{2k}} \sum_{r|k} \mu(r) q^{\frac{k}{r}} = \sum_{r=1}^{\infty} \frac{\mu(r)}{r} \sum_{l=1}^{\infty} \frac{1}{lq^{2rl-l}}.$$

Taking in account that

$$\sum_{k=1}^{\infty} \frac{x^k}{k} = \log\left(\frac{1}{1-x}\right),$$

we get

$$\gamma(q) = \sum_{r=1}^{\infty} \frac{\mu(r)}{r} \log\left(\frac{q^{2r-1}}{q^{2r-1}-1}\right).$$

Therefore, expanding the first five terms and recalling that $\mu(r) \leqslant 1$ and $\mu(4) = 0$, we derive

$$\begin{aligned}\gamma(q) &= \log\left(\frac{q}{q-1}\right) - \frac{1}{2}\log\left(\frac{q^3}{q^3-1}\right) - \frac{1}{3}\log\left(1 + \frac{1}{q^5-1}\right) \\ &\quad - \frac{1}{5}\log\left(1 + \frac{1}{q^9-1}\right) + \sum_{r=6}^{\infty} \frac{\mu(r)}{r} \log\left(\frac{q^{2r-1}}{q^{2r-1}-1}\right) \\ &\leqslant \log\left(\frac{q}{q-1}\right) - \frac{1}{2}\log\left(\frac{q^3}{q^3-1}\right) + \frac{1}{6}\sum_{r=6}^{\infty} \log\left(\frac{q^{2r-1}}{q^{2r-1}-1}\right).\end{aligned}$$

Recalling that if $0 \leqslant x \leqslant \frac{1}{2}$ then $\log(\frac{1}{1-x}) \leqslant \frac{x}{1-x} \leqslant 2x$ and putting $x = \frac{1}{q^{2r-1}}$ we have

$$\begin{aligned}\gamma(q) &\leqslant \log\left(\frac{q}{q-1}\right) - \frac{1}{2}\log\left(\frac{q^3}{q^3-1}\right) + \frac{1}{6}\sum_{r=6}^{\infty}\frac{1}{q^{2r-1}-1} \\ &\leqslant \log\left(\frac{q}{q-1}\right) - \frac{1}{2}\log\left(\frac{q^3}{q^3-1}\right) + \frac{1}{3}\sum_{r=6}^{\infty}\frac{1}{q^{2r-1}} \\ &= \log\left(\frac{q}{q-1}\right) - \frac{1}{2}\log\left(1+\frac{1}{q^3-1}\right) + \frac{1}{3q^9(q^2-1)}.\end{aligned}$$

For $q \geqslant 2$ we have

$$\frac{1}{2}\log\left(1+\frac{1}{q^3-1}\right) = \frac{1}{2}\left(\frac{1}{q^3-1}\right)\log\left(1+\frac{1}{q^3-1}\right)^{q^3-1}$$

$$\geqslant \frac{7}{2}\left(\frac{1}{q^3-1}\right)\log\left(\frac{8}{7}\right) > \frac{1}{q^9}\cdot\frac{7}{2}\log\left(\frac{8}{7}\right) > \frac{1}{q^9}\cdot\frac{1}{3(2^2-1)} \geqslant \frac{1}{3q^9(q^2-1)}$$

and the result follows. □

We have already remarked that for any choice $u_1, \ldots, u_m$, $v_1, \ldots, v_m$, $d = \gcd(a_1, \ldots, a_m)$ divides $D = \gcd(\sum_{j=1}^m u_j a_j, \sum_{j=1}^m v_j a_j)$, thus $\deg d \leqslant \deg D$, and $\deg d = \deg D$ if and only if $d = D$, because d and D are both monic polynomials.

Therefore if executing our algorithm twice we get two different probabilistic gcd's with different degree, it is trivial that which has higher degree is incorrect, whereas if we get two different probabilistic gcd's with the same degree, then they are both incorrect.

So recalling $\log(\frac{q}{q-1}) \to \frac{1}{q}$ for $q \to \infty$ we see that performing finitely k times our algorithm we have that asymptotically the probability of a failure exponentially decreases as q^{-k}.

We explicitly state the algorithm using a pseudo-code.

Algorithm 1. Probabilistic gcd of many polynomials over a finite field.

Input: $q \geqslant 2$ *a prime power*, $a_1, \ldots, a_m \in \mathbb{F}_q[X]$ *non-zero polynomials with degree at most n such that the maximum degree is taken by only one polynomial*, $s \geqslant 1 + \log_q n$, $0 < \varepsilon < 1$ *the error tolerance*.

Output: D, *probabilistic* $\gcd(a_1, \ldots, a_m)$ *with probability at least* $1 - \varepsilon$.

- *Compute*

$$k = \left\lceil \frac{\log \varepsilon}{\log[\log(\frac{q}{q-1}) + \frac{2}{sq}]} \right\rceil,$$

  the number of iterations.
- $D \leftarrow a_1$.
- $j \leftarrow 1$.

- **While** $j \leqslant k$ **and** $D \neq 1$ **do**
  (1) *Select independently and uniformly distributed random polynomials* $u_1, \ldots, u_m, v_1, \ldots, v_m$ *from* $\mathscr{M}_s$, *and compute*

$$\bar{D} = \gcd\left(\sum_{j=1}^{m} u_j a_j, \sum_{j=1}^{m} v_j a_j \right).$$

  (2) **If** $\deg \bar{D} < \deg D$ **then** $D \leftarrow \bar{D}$.
  (3) $j \leftarrow j + 1$.
- **Return** D, *probabilistic* $\gcd(a_1, \ldots, a_m)$ *with probability at least* $1 - \varepsilon$.

We remark that if $q = 2$ then choosing $s \geqslant \max\{1 + \log_2 n, 146\}$ we get that after two iterations of the algorithm the probability of success becomes greater of $\frac{51}{100}$.

3. Remarks

We have already mentioned that there are other ways of reduction this computation.

The first one is described and analyzed in Section 6.9 of [3] (as well as [2]); in particular, it shown in Theorem 6.45 of [3] that, for any set T of $\#T = M$ elements from $\mathbb{F}_q$ or its extension, if one selects $m - 2$ elements $t_3, \ldots, t_m \in T$ uniformly at random then for any $m \geqslant 3$ non-zero polynomials $a_1, \ldots, a_m \in \mathbb{F}_q[X]$ of degree at most n

$$\gcd\left(a_1, a_2 + \sum_{j=3}^{m} t_j a_j \right) = \gcd(a_1, \ldots, a_m)$$

with probability

$$P \geqslant 1 - \frac{n}{M}.$$

Obviously for this algorithm to be non-trivial, say to guarantee $P \geqslant \frac{1}{2}$, the field should contain at least $2n$ elements. Thus for a small q one have to construct and work in an extension of $\mathbb{F}_q$ of degree r of order $\log n$.

It is easy to see that the cost of computation of the linear combinations

$$\sum_{j=3}^{m} t_j a_j \quad \text{and} \quad \sum_{j=1}^{m} u_j a_j$$

for elements $t_3, \ldots, t_m \in \mathbb{F}_{q^r}$ and for polynomials $u_1, \ldots, u_m \in \mathscr{M}_s$, where both r and s are of order $\log n$, respectively takes

$$O(mn \log n)$$

arithmetic operations in $\mathbb{F}_q$ for the first linear combination, and

$$O(mn(\log\log n)(\log\log\log n))$$

arithmetic operations in $\mathbb{F}_q$ for the second one.

Furthermore, after this computation the algorithm of [3] computes the greatest common divisors of two polynomials of degree at most n over $\mathbb{F}_{q^r}$ while the algorithm of this paper computes the greatest common divisors of two polynomials of degree at most $n + O(\log n)$ over $\mathbb{F}_q$, which is at least r times faster. Now we assume that one uses:

- Fast implementation of $\mathbb{F}_{q^r}$ arithmetic operations via $\mathbb{F}_q$ arithmetic, so each $\mathbb{F}_{q^r}$ operation takes $O(r(\log r)(\log\log r))$ $\mathbb{F}_q$ operations, see Corollary 9.7 from [3] (one also recalls the representation

$$\mathbb{F}_{q^r} \cong \mathbb{F}_q[Y]/f(Y),$$

  where f is an irreducible polynomial over $\mathbb{F}_q$ of degree r, see [4]).
- the fast Euclidean algorithm to compute the greatest common divisor algorithm of two polynomials of degree at most N which takes
  $O(N(\log N)^2(\log\log N))$ arithmetic operations in the field of the definition of the polynomials, see Theorem 8.19 from [1] as well as Corollary 11.6 from [3].

Then the total cost is

$$O(mn(\log n) + n(\log n)^3(\log\log n)^2(\log\log\log n))$$

for the algorithm of [3], and

$$O(mn(\log\log n)(\log\log\log n) + n(\log n)^2(\log\log n))$$

for the algorithm of this paper, thus we always have an asymptotic improvement.

If one uses classic arithmetic, which is probably the case in many practical implementations, then the cost of the second part is $O(n^2)$ for our algorithm and is $O(n^2(\log n)^2)$ for the algorithm of [3] (for example, see Theorem 6.46 of [3]) and our algorithm always exhibits better asymptotic complexity.

A second method to reduce this computation is described and analyzed in [5]; namely it is shown that if $\gamma_j^{(l)}$ are chosen uniformly and randomly from $\{0,1\}$, then

$$\gcd\left(a_1, \sum_{j=1}^{m} \gamma_j^{(1)} a_j, \ldots, \sum_{j=1}^{m} \gamma_j^{(k)} a_j\right) = \gcd(a_1, \ldots, a_m)$$

holds with probability

$$P(k) \geqslant 1 - \frac{n}{2^k},$$

independent of q.

Therefore the algorithm of [5] saves on the computational cost of the linear combinations, but, fixed an error tolerance $0 < \varepsilon < 1$, in order to have the probability of success at least $1 - \varepsilon$ it needs much more pairwise greatest common divisors computations than the algorithm of this paper. Namely, it requires to compute $\log_2(\frac{n}{\varepsilon})$ pairwise greatest common divisors, whereas the algorithm of this paper requires to compute $O(\log_q(\frac{1}{\varepsilon}))$ pairwise greatest common divisors.

Hence our algorithm exhibits a lower computational complexity when the cost of computation of the greatest common divisor dominates the cost of computation of the linear combinations.

Acknowledgments

The author sincerely thanks Igor Shparlinski for suggesting this problem and his helpful advice, and Macquarie University for offering him a shelter during the preparation of this paper.

Warm thanks are also due to the anonymous referee for his/her careful reading of the manuscript, pointing out Refs. [5,6], and his/her valuable suggestions.

References

[1] A.V. Aho, J.E. Hopcroft, J.D. Ullman, The Design and the Analysis of Computer Algorithms, Addison-Wesley, Reading, MA, 1974.

[2] G. Cooperman, S. Feisel, J. von zur Gathen, G. Havas, GCD of many integers, Proceedings of the Fifth International Computing and Combinatorics Conference, Tokyo, 1999, Lecture Notes in Computer Science, Vol. 1627, Springer, Berlin, 1999, pp. 310–317.

[3] J. von zur Gathen, J. Gerhard, Modern Computer Algebra, Cambridge University Press, Cambridge, 1999.

[4] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.

[5] T. Mulders, A. Storjohann, Diophantine linear system solving, Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (ISSAC), Vancouver, ACM Press, New York, 1999, pp. 181–188.

[6] T. Mulders, A. Storjohann, Certified dense linear system solving, Technical Report 355, Department of Computer Science, ETH Zurich, December 2000.